REMARKS

Applicants have amended claims 5-7, 10-12, 19, 22, 25, 28, and 31-32 and have canceled claims 1-4, 8-9, 13-18, 20-21, 23-24, 26-27, and 29-30 during prosecution of this application. Applicants are not conceding in this application that said amended and canceled claims are not patentable over the art cited by the Examiner, since the claim amendments and cancellations are only for facilitating expeditious prosecution of the patent application. Applicants respectfully reserve the right to pursue said amended and canceled claims, and other claims, in one or more continuations and/or divisional patent applications.

In a telephonic interview held 05/22/2007 between Applicants' Representative Jack P. Friedman and Examiner Matthew T. Henning:

(1) a proposed modification in independent claim 5 of the feature: "for each occurrence of the value of the signature event counter exceeding the signature threshold quantity" was discussed and it was agreed not to pursue said proposed modification;

(2) the Examiner will review additional proposed modifications of claim 5 (in light of the prior art) after formal submission of Applicants' next office action response to office action mailed 02/26/2007 and agreed to contact Applicants' Representative if such contact would expedite prosecution of the present patent application;

(3) Applicants' Representative requested that the Examiner focus particular attention on amended claim 31 in addition to amended claim 5 in Applicants' next office action response , and the Examiner agreed to do so.

The Examiner rejected claims 5, 10 and 19-30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Vaidya (US Patent Number 6,279,113)and further in view of Sharma *et al.* (US Patent Number 6,909,692) hereinafter referred to as Sharma.

The Examiner rejected claims 6 and 11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

The Examiner rejected claims 7 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Martin *et al.* (US Patent Number 6,772,349) hereinafter referred to as Martin.

The Examiner rejected claims 31-32 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above, and further in view of Narendran *et al.* (US Patent Number 6,070,191) hereinafter referred to as Narendran.

Applicants respectfully traverse the § 103 rejections with the following arguments.

35 U.S.C. §103(a): Claims 5, 10, and 19-30

The Examiner rejected claims 5, 10 and 19-30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Vaidya (US Patent Number 6,279,113)and further in view of Sharma *et al.* (US Patent Number 6,909,692) hereinafter referred to as Sharma.

Since claims 20-21, 23-24, 26-27, and 29-30 have been canceled, the rejection of claims 20-21, 23-24, 26-27, and 29-30 under 35 U.S.C. § 103(a) is moot.

Applicants respectfully contend that claims 5 and 10 are not unpatentable over Vaidya in view of Sharma, because Vaidya in view of Sharma does not teach or suggest each and every feature of claims 5 and 10.

As a first example of why Vaidya in view of Sharma does not teach or suggest the following combination of features of claims 5 and 10:

> "wherein the intrusion detection system comprises an intrusion detection server and an intrusion detection sensor,
>
> wherein the intrusion detection sensor is coupled to the intrusion detection server and to the protected device,
>
> wherein the intrusion detection sensor comprises a governor, a programmable processor that oversees operation of the intrusion detection sensor, and a signature file,
>
> wherein the governor includes a log, a timer, an alert generation rate threshold, and one or more rules that prescribe actions to be taken in order to decrease the generation rate of alerts by the intrusion detection sensor when the present alert generation rate exceeds the alert generation rate threshold,
>
> wherein operation of the timer, utilization of the alert generation rate threshold, and implementation of the one or more rules are carried out by instructions executed by the programmable processor,

> wherein the log consists of a list of timestamps that record the times at which the intrusion detection sensor generates alerts,
>
> wherein the signature file includes a signature set comprising elements that include a signature set identifier, a signature event, a signature event counter that keeps count of the number of occurrences of the signature event, a signature threshold quantity, and a signature threshold interval, and
>
> wherein the signature event includes a bit pattern that identifies the signature event".

As a second example of why Vaidya in view of Sharma does not teach or suggest the following of feature of claims 5 and 10: "adjusting the value of the signature event counter to not include a count of signature events past a sliding window specified by the signature threshold interval".

As a third example of why Vaidya in view of Sharma does not teach or suggest the following combination of features of claims 5 and 10:

> "for each occurrence of the value of the signature event counter exceeding the signature threshold quantity:
>
> generating an alert by the intrusion detection sensor;
>
> after said generating, recording in the log a timestamp denoting a time of generating the alert, said time of generating the alert derived from the timer;
>
> after said recording, clearing the log of any entries that are past a permissible age, said permissible age equal to a ratio of a cap imposed by the governor upon a rate of generation of alerts by the intrusion detector sensor to the alert generation rate threshold;
>
> after said clearing, determining from contents of the log the present alert generation rate, said determining the present alert generation rate comprising dividing the number of timestamps in the log by the permissible age;

after said determining, comparing the present alert generation rate with the alert generation rate threshold, said comparing ascertaining that the present alert generation rate exceeds the alert generation rate threshold;

responsive to said ascertaining that the present alert generation rate exceeds the alert generation rate threshold, altering an element of the signature set to decrease a rate at which alerts are generated by the intrusion detection sensor, said altering the element being implemented in accordance with said one or more rules."

Based on the preceding arguments, Applicants respectfully maintain that claims 5 and 10 are not unpatentable over Vaidya and further in view of Sharma, and that claims 5 and 10 are in condition for allowance. Since claims 19 and 22 depend from claim 5, Applicants contend that claims 19 and 22 are likewise in condition for allowance. Since claims 25 and 28 depend from claim 10, Applicants contend that claims 25 and 28 are likewise in condition for allowance.

35 U.S.C. §103(a): Claims 6 and 11

The Examiner rejected claims 6 and 11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

Since claims 6 and 11 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 6 and 11 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Lunt under 35 U.S.C. §103(a).

35 U.S.C. §103(a): Claims and 12

The Examiner rejected claims 7 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Martin *et al.* (US Patent Number 6,772,349) hereinafter referred to as Martin.

Since claims 7 and 12 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 7 and 12 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Martin under 35 U.S.C. §103(a).

35 U.S.C. §103(a): Claims 31 and 32

The Examiner rejected claims 31 and 32 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above, and further in view of Narendran *et al.* (US Patent Number 6,070,191) hereinafter referred to as Narendran.

Since claims 31 and 32 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 31 and 32 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Narendran under 35 U.S.C. §103(a).

In addition, Applicants respectfully maintain that the combination of Vaidya and Sharma does not teach or suggest the feature: "for each scheduled update time occurrence: clearing the log of any entries that are past the permissible age, determining from contents of the log the current alert generation rate by dividing the number of timestamps in the log by the permissible age".

Accordingly, Applicants respectfully maintain that claims 31 and 32 are not unpatentable over Vaidya in view of Sharma and further in view of Narendran under 35 U.S.C. §103(a).

CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Date: 05/22/2007

Jack P. Friedman

Jack P. Friedman
Registration No. 44,688

Schmeiser, Olsen & Watts
22 Century Hill Drive - Suite 302
Latham, New York 12110
(518) 220-1850